Playing with Lives: Cyberattacks on Healthcare are Attacks on People

March 2021

Executive Summary

Online or offline, **attacking healthcare is attacking people**. **As a critical and often vital service provider**, **healthcare should be off-limits to any malicious intent or action**, **safeguarded for and by all**, **at all times**, **in conditions ensuring that human security**, **dignity and equity are respected in digital ecosystems**. **Conditions that we call cyberpeace**.

In stark contrast to such conditions, since November 2020, the number of global cyberattacks against the healthcare sector has increased by 45%, compared to an average of 22% in other sectors[1]. In November 2020 alone, healthcare organizations in all regions of the world experienced a significant rise in the number of cyberattacks, with Central Europe, East Asia and Latin America suffering over twofold increases[2].

This Report is a cornerstone of the Cyber 4 Healthcare program that the CyberPeace Institute launched in 2020 to assist healthcare professionals analyse attacks and advance policies to protect the sector and the people it serves. Our objectives are to de-escalate the number and magnitude of cyberattacks, enforce the responsibility and accountability of all actors and ensure that victims have a voice and the right to redress.

Consolidating information that demonstrates the complexity, magnitude and scope of the global cyber threat to healthcare, **this Report focuses for the first time on the impacts of attacks on people and society**. On the basis of victims' testimonials, cybersecurity reporting, volunteer initiatives, legal frameworks and empirical research, it analyses the technical innovation of modus operandi, the diversity of threat actors and their motivations, the difficult implementation of domestic and international norms and laws, and the under-resourcing of the sector despite a vibrant ecosystem of assistance initiatives. From ransomware through to COVID-19 disinformation operations, as incidents are underreported, attacks seldomly attributed and threat actors act with impunity, the Report shows how accountability is critical to any systemic solution.

[1] Check Point Software (2021) 'Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again', Check Point Software, 5 January. Available at: https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/ (Accessed: 12 January 2021).

[2] ibid

Recommendations

Online or offline, **attacking healthcare is attacking people**. Throughout this Report, we aim to show that while healthcare professionals and patients are facing a significant, evolving and compounding threat, **collective action is possible**. The Report shows the overarching responsibilities of nation states in leading the way to decrease attacks globally and to hold threat actors accountable.

These recommendations are addressed to governments, industry, the healthcare sector, academia and civil society, with the aim of securing long-lasting impact by reducing attacks on healthcare. The recommendations propose to:

1 Document attacks and analyse their human and societal impact

2 Improve the healthcare sector's preparedness and resilience to:

2.1 Strengthen the cybersecurity of healthcare infrastructure

2.2 Increase healthcare capacity and capabilities

2.3 Improve healthcare preparedness to attacks

3 Activate technical and legal instruments to protect healthcare to:

3.1 Reinforce the legal and normative ecosystem

3.2 Improve information-sharing and reporting standards

4 Hold threat actors to account

The CyberPeace Institute commits to supporting the recommendations through the:

- **Continuous monitoring, documentation and dissemination of information on attacks on healthcare and on the application or violation of laws, norms and regulations,**
- **Collection of victim testimonials, and**
- **Support and development of assistance initiatives.**

It will also cooperate with partners to conduct vulnerability analysis and risk assessments so as to precisely define and evaluate shortfall in the human, financial, government, technical and insurance resources needed to secure the complex and critical healthcare infrastructure. Through the application of a designated accountability framework, accountability in cyberspace will be tracked and recorded to reduce cyber threat to the healthcare sector.

The CyberPeace Institute will campaign globally and engage all stakeholders around a simple goal – that every healthcare professional, patient and person around the world has the right to benefit from healthcare without fear or harm, both during times of conflict and during times of peace.

Why is the healthcare sector under attack?

Financially and politically motivated attacks on healthcare exploit vulnerabilities in the sector's fragile digital infrastructure and weaknesses in its cybersecurity regime.

The healthcare sector has long been a target of attacks. However, the COVID-19 pandemic has further exacerbated the sector's threat landscape, exposing it to a convergence of threats that can be attributed to three key factors:

- Healthcare has become a target of choice for disruptive digital extortion attacks due to its **responsibility to maintain critical systems to ensure public health**. The imperatives of meeting vital human needs make it a uniquely vulnerable, hence lucrative target for ransomware attacks.
- Healthcare organizations are **custodians of valuable data**. Whereas medical records are among the most profitable data on underground markets, sold for up to USD 250 per record, medical research has proven to be of strategic value, especially during the pandemic.
- The healthcare sector's **strategic positioning** during the COVID-19 pandemic has placed it at the center of inter-state rivalries. Consequently, competing states have sought to undermine rival states' pandemic responses by targeting healthcare and the trust that people place in it.

These threats are facilitated by the sector's **fragile digital infrastructure** and its pervasive **underinvestment in cybersecurity**. Healthcare has been pressed to adopt rapid digitalization, and thereby also a rapidly growing attack surface. While some healthcare organizations have adjusted to these changes by implementing adequate cybersecurity programs, much of the sector continues to suffer from a systemic lack of resources and trained personnel to secure its often complex and outdated infrastructure. The sector will remain a target of choice and opportunity if its vulnerabilities are not addressed.

What is the real impact of attacks on healthcare?

Attacks on healthcare are causing direct harm to people and are a threat to health and life, globally.

The convergence of attacks on the sector's digital infrastructure, on its pandemic response, and on the trust in the sector's ability to function as needed is creating a **global threat to health and human life**. While the targets of attacks are most often portrayed as the healthcare organizations or service providers whose data or infrastructure was compromised (including but not limited to hospitals and healthcare service providers, pharmaceutical companies and government health ministries), the actual direct victims of attacks are healthcare professionals, patients and society as whole, who suffer in the long term. While the phenomenon is under-researched, the documented impacts of converging threats are of immediate and pressing concern.

Disruptive attacks on hospitals and medical service providers have a **physical impact on people**. Ransomware-hit hospitals have been forced to delay surgeries, reroute incoming ambulances, and revert to more time-consuming processes. Such attacks can have an impact on a hospital's ability to provide efficient services in the long term, as demonstrated by a study that observed a higher mortality rate among hospitals that had suffered a data breach within the past three years[3]. In the times of the COVID-19 pandemic, the disruption of medical services can negatively influence not only the course of a patient's illness but also the spread of the virus.

The psychological impact of attacks is much less immediately visible but causes significant suffering nevertheless. During a disruptive attack healthcare professionals experience increased levels of stress and anxiety from being in an incident response situation while fear and a sense of coercion, lack of control and powerlessness prevail when ransom demands are made. Following a data breach, trust in the healthcare sector is eroded and patients can experience feelings of violation, betrayal and heightened insecurity when cybercriminals use stolen data to engage in identity theft. On a much broader level, attacks impacting supply chains destabilize confidence in the healthcare sector's technical environment.

While the direct impact of attacks on healthcare may differ from one incident to another, **the societal impact** is very much the same. Whether through the breach of confidential medical records, the disruption of medical services, or the dissemination of COVID-19 disinformation, attacks against the healthcare sector generate a **climate of fear, confusion and distrust**. In turn, this impedes the sector's ability to respond in times of public health crises and affects the public's decision to seek optimal treatment.

The business and economic impact of attacks on healthcare has lasting effects for several years after the attack itself and their costs can be less tangible and difficult to measure. Following an attack, healthcare organizations suffer from a time-consuming and often exorbitant recovery process, requiring contingency funding to recover and improve its systems, cover regulatory penalties, re-train staff, and manage reputational damage. In some cases, such costs may include a ransom payment which is strongly discouraged for its likelihood to incite similar extortive demands in the future, with no guarantee that the ransom payment will yield the outcome sought.

[3] Choi, S. J., Johnson, M. E. and Lehmann, C. U. (2019) 'Data breach remediation efforts and their implications for hospital quality', Health Services Research, 54(5), pp. 971–980. doi: 10.1111/1475-6773.13203.

How are healthcare attacks unfolding and evolving?

Cyberattacks are increasing as the arsenal of weapons used to target healthcare is evolving.

Further to the steady rise in cyber threats to healthcare in the past few years, the world has seen a striking escalation and evolution of three key cyber threats against healthcare during the COVID-19 pandemic:

Disruptive attacks have affected healthcare globally, with ransomware posing a particular threat due to its ability to deliver vital healthcare services. Whether by chance or opportunity, ransomware operations have evolved drastically in 2020 through adoption of double extortion tactics, which not only encrypt but also threaten to leak healthcare data. These tactics and their evolution have been exacerbated by expanding collusion among cybercriminal actors seeking to maximize their efficiency and profits. Further evolution of this attack type can be expected through its amplification with other attack types (e.g. DDoS) or the monetization of stolen healthcare data (e.g. the extortion of healthcare data subjects, sale of medical records). Ransomware creates both an immediate risk to patient care and a long-lasting impact on healthcare organizations.

Healthcare data breaches resulting from cyberattacks have increased substantially around the world over the course of the pandemic, with the US seeing a 39% increase from 2019 to 2020[4]. Pandemic-induced developments such as remote work and a surge in telehealthcare owing to social distancing measures have undoubtedly increased the threat surface for healthcare data. Specifically, the global emergency situation has elevated the value of COVID-19-related data, both financially and strategically. As a result, healthcare is not only being increasingly targeted by cybercriminals aiming to monetize healthcare data but also by state actors seeking to gain a strategic advantage in the race to vaccine research and development or pandemic-response capabilities.

Disinformation operations have targeted healthcare both directly and indirectly, exploiting and contributing to the ambiguity of the COVID-19 Infodemic. State actors have allegedly stolen, manipulated, and disseminated information from organizations involved in the pandemic response or the development of COVID-19 vaccines. By manipulating and leaking authentic information, the threat actors lend credibility to their disinformation narratives. Such cyber-enabled information operations threaten to undermine people's trust in healthcare organizations and ultimately may impede the pandemic response.

[4] U.S. DoHHS (no date) Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Department of Health & Human Services - Office for Civil Rights. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Accessed: 17 February 2021).

Who are the prevalent threat actors?

Attacks on healthcare are low-risk, high-reward crimes. Acting with near impunity, criminals and state actors are joining forces against healthcare with varying motives and agendas.

Two types of threat actors pose the greatest danger to the healthcare sector: cybercriminals and state actors. The line is increasingly blurred between the two as **state-sponsored / funded proxies** who act on behalf of states have emerged in recent years, further complicating the attribution of attacks.

Cybercriminals pose a high-risk, high-impact threat to the healthcare sector. Motivated primarily by financial gain, cybercriminals and more specifically ransomware operators have attacked healthcare organizations during the pandemic despite pledging not to attack hospitals. The COVID-19 pandemic also enabled a context in which often highly sophisticated **state actors** seek to shift the realities of global geopolitics as they commit attacks by compromising, stealing, altering or destroying information. Since March 2020, state-sponsored cyberespionage groups have targeted vaccine research, development, and testing facilities in an attempt to gain a competitive edge.

All types of threat actors attacking healthcare have been able to operate with near impunity. The enforcement and prosecution rate for perpetrators of attacks on healthcare is extremely low. This stems notably from the underreporting of attacks, from the lack of resources in law enforcement and the judiciary, and from shortfalls in attribution. Moreover, opportunities offered by legal instruments, such as investigative cooperation, and enforcement mechanisms, such as sanctions, are rarely used systematically in the case of cyberattacks against healthcare and are rendered still more complex by geopolitical agendas in the case of state or state-sponsored attacks.

What instruments are available to protect healthcare from attacks?

States are not availing themselves of the full extent of norms and laws available to protect healthcare.

Attacks on the healthcare sector have radically increased during the COVID-19 pandemic in parallel to the urgency of the health crisis and they have dire consequences on the exercise of fundamental rights. A general reluctance to apply legal and normative frameworks has left the sector more vulnerable. **Many instruments and opportunities** – ranging from domestic law to international law to voluntary non-binding norms – are available to hold threat actors accountable for their actions, to protect critical infrastructure and better secure digital products.

Regrettably, these opportunities also come with corresponding **challenges**. Within the UN-mandated processes (UN GGE and UN OEWG) and multistakeholder initiatives (i.e. Paris Call), governments have not stated unanimously that medical and healthcare facilities must never be targeted and consistently protected against cyberattacks. Moreover, there are no international agreements on thresholds for applying the principles of international law, and voluntary non-binding norms are not consistently implemented.

These challenges ultimately inhibit a nation state's ability to address impunity in cyberspace. This is exacerbated by the lack of capacity of national law enforcement agencies and the judiciary to act in the event of extraterritorial cases. Such deficits underscore the need for greater accountability and enforcement in cyberspace.

Industry actors can better apply multistakeholder norms to protect healthcare.

Multistakeholder norms, such as those put forth by the Paris Call Principles, the Cybersecurity Tech Accord, and the Charter of Trust offer important and helpful insights into how industry actors can better protect healthcare. Implementing security-by design, reporting vulnerabilities, especially those in critical infrastructure, and advancing user protection through tangible action are timely measures capable of addressing some of the urgent threats against the healthcare sector. Making these norms standard procedure, via binding frameworks, would contribute substantially to affording adequate protection to users, critical infrastructure providers and critical suppliers.

Could a strong accountability framework increase responsible behavior in cyberspace?

There is today no transparent and independent mechanism to track accountability in cyberspace.

The CyberPeace Institute has identified that **closing the accountability gap** is a prerequisite to establishing cyberpeace and securing the protection of vulnerable communities, particularly so in the current absence of any systematic documentation or transparency on how malicious actors are violating laws, norms and principles.

Closing the accountability gap implies more than attribution alone. It also involves identifying roles and responsibilities of all stakeholders involved as well as the applicable laws, norms, and principles required to ensure security, dignity, and equity in cyberspace. The CyberPeace Institute's accountability framework proposes a model by which the expectations and commitments of all stakeholders in cyberspace are mapped against their level of adherence to these commitments and the consequences of failing to uphold them.

Inasmuch as software vendors, manufacturers, healthcare organizations, and practitioners bear a responsibility in securing the healthcare infrastructure, nation states are able to operate across the technical, ethical, judicial, and normative levels, and can establish and enforce responsibilities through regulation and the application of law and order. States have the unique power and, arguably, responsibility to lead the way in achieving and maintaining cyberpeace for healthcare. A strong and binding accountability framework could pave the way for this.

How are different stakeholders joining forces in support of the healthcare sector?

Assistance initiatives lack visibility, scale and sustainability.

Just as cybercriminals and other threat actors have joined forces to attack healthcare, numerous coalitions have arisen to protect it by providing fast and free support. They include:

- **Resilience initiatives** to help healthcare organizations prevent and defend against attacks through awareness-raising, information-sharing and the provision of tools and services.
- **Response initiatives** to provide cybersecurity and technical expertise in times of crisis to help in investigating the threat and secure infrastructure.
- **Victim-support initiatives** to provide practical and psychological assistance to victims following cyberattacks.

Civil society organizations, governments, private firms, academia, and international organizations as well as cybersecurity practitioners from around the world are operating within agile and targeted assistance models while public-private, private-private and volunteer networks proliferate. These initiatives have often lacked visibility, scale, and sustainability but have proven that a variety of actors are willing to protect healthcare and that **collective action is possible**.

Conclusion

The Report is an initial endeavour to identify and assess the systemic cybersecurity issues confronting healthcare, and cyberspace more broadly. The analysis has also identified a gap in the accessibility and availability of data on healthcare attacks, their scale, and real impact. There is today no global standard for reporting attacks, collecting attack data, and sharing information. Likewise, and arguably as a result, there is little empirical research on the short- and long-term impact of cyberattacks on healthcare and society, notably on patient care. **There can be no response without knowledge**. The recommendations proposed in this Report seek to bridge the knowledge gap and the CyberPeace Institute commits to driving collective responses to the cyber challenges of our day.

The victims of attacks against healthcare are varied and international but nonetheless interconnected. Threat actors, regardless of their motive, are endangering lives and the overall ability of the sector to provide crucial services. Addressing this issue will require the closing of the accountability gap, whereby accountability and responsibility does not lie with a single entity but with all concerned stakeholders. Through a collective and coordinated response, trust and security in the healthcare sector will prevail over fear and harm.

Executive Summary

Report